AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method for calculating hashing of a message in a device communicating with a smart card, comprising:

storing a same hash function in said device and said smart card, wherein the message is divided in data blocks and comprises ~~data blocks including secret data~~ keys and ~~other~~ public data, and wherein ~~secret data~~ the keys are ~~is~~ only known by the smart card;

performing a calculation of the hash function of ~~secret data~~ the keys in the smart card; and

performing the calculation of the hash function of all or part of other ~~public~~ data of the message in the device, wherein the other data is public data.

2. (Currently Amended) The method according to claim 1, wherein, if ~~secret data~~ the keys are [[is]] followed by ~~other~~ public data in the message, the smart card starts the calculation of the hash function of all blocks that include ~~secret data~~ the keys and then sends a corresponding intermediate result to the device, which [[that]] continues the calculation of the hash function by using the intermediate result and ~~other~~ the public data.

3. (Canceled)

4. (Currently Amended) The method according to claim 1, wherein, if the public data is followed by ~~secret data~~ the keys, the device starts performing the calculation of the hash function of the public data and then sends [[the]] a corresponding intermediate result and a remaining part of last hash block to the smart card, which [[that]] continues to perform the calculation of the hash function internally by using the corresponding intermediate result, the remaining part of last hash block, and ~~secret data~~ the key.

5. (Currently Amended) An apparatus comprising:

a communication device configured to be coupled to a smart card, said communication device and said smart card storing a same hash function for calculating a hash of a

message[[;]], [[a]]said message being divided in data blocks and comprising ~~data blocks including secret data~~ keys and ~~other~~ public data, wherein the keys are ~~secret data is~~ only known by the smart card,

wherein said communication device includes a program for performing the following steps:

a hashing step in which all or part of said ~~other~~ public data is hashed in said communication device, and

a requesting step in which, said communication device requests the smart card to perform [[the]] calculation of the hash function of the keys ~~secret data~~.

6. (Currently Amended) An apparatus comprising:

a smart card coupled to a communication device for calculating a hash function of a message, said communication device and said smart card storing a same hash function, wherein [[a]]said message is divided in data blocks and comprises keys ~~data blocks including secret data~~ and ~~other~~ public data, wherein the keys are ~~secret data is~~ only known by the smart card, wherein said smart card includes a program for performing upon a request from said communication device a calculation of the hash function of the keys of the message ~~the following steps:~~

~~a hashing step in which all or part of said other public data is hashed in said communication device, and~~

~~a requesting step in which, said communication device requests the smart card to perform the hash function of the secret data~~.

7. (New) An system comprising:

a smart card; and

a communication device configured to be coupled to said smart card, said communication device and said smart card storing a same hash function for calculating a hash of a message, said message being divided in data blocks and comprising keys and public data, wherein the keys are only known by the smart card,

wherein said communication device includes a program for performing the following steps:

a hashing step in which all or part of said public data is hashed in said communication device, and

a requesting step in which, said communication device requests the smart card to perform calculation of the hash function of the keys, and

wherein said smart card includes a program for performing, upon a request from said communication device, calculation of the hash function of the keys of the message.